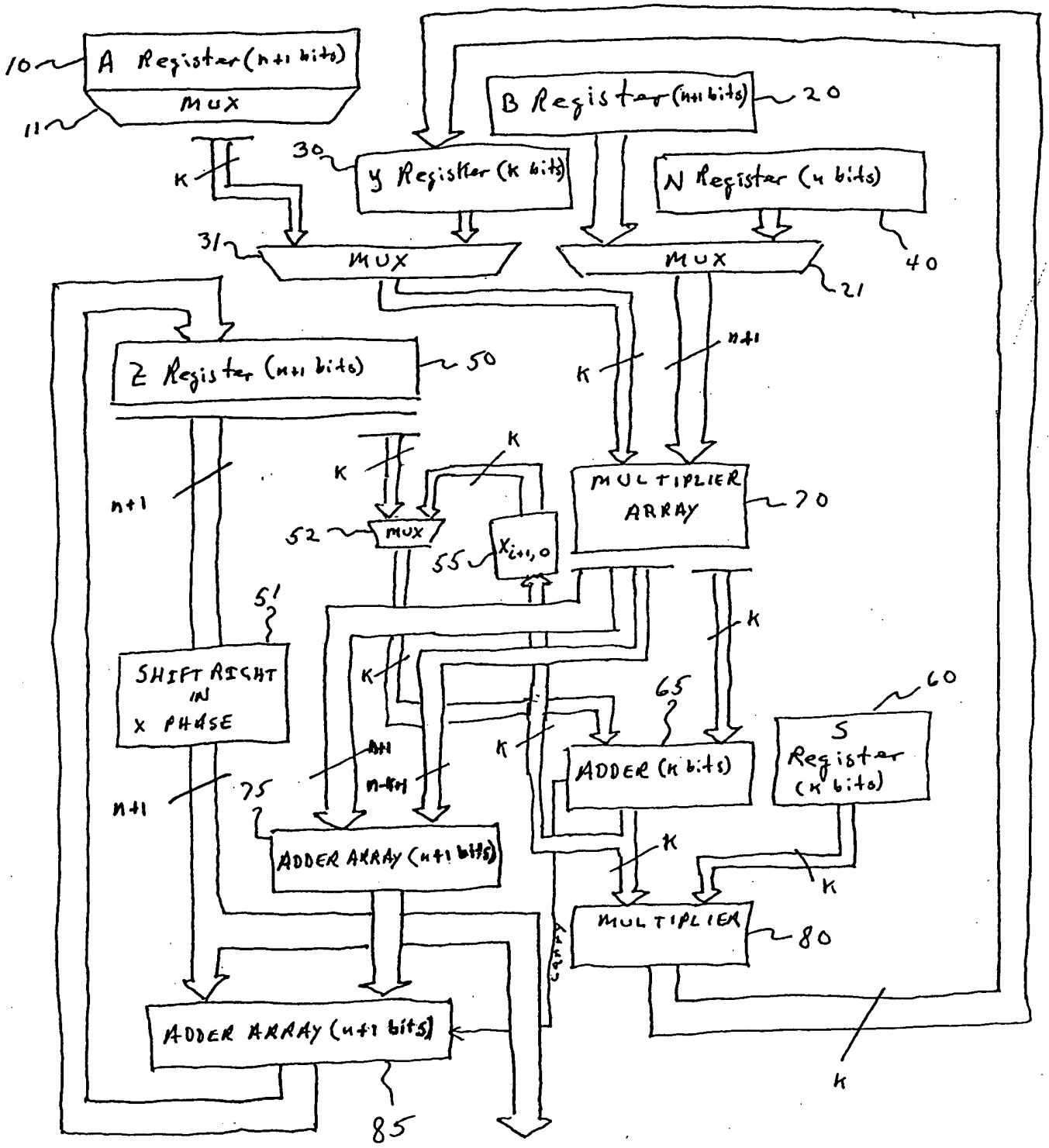
10
A Register (n+1 bits)
MUX
11
B Register (n+1 bits)
20
30
y Register (K bits)
N Register (n bits)
K
31
MUX
MUX
21
40
Z Register (n+1 bits)
50
K
n+1
K
K
n+1
MULTIPLIER ARRAY
70
52
MUX
55
$X_{i+1,0}$
51
SHIFT RIGHT IN X PHASE
K
65
60
S Register (K bits)
ADDER (K bits)
n+1
n-K+1
75
n+1
ADDER ARRAY (n+1 bits)
K
K
MULTIPLIER
80
ADDER ARRAY (n+1 bits)
85
K

Figure 1

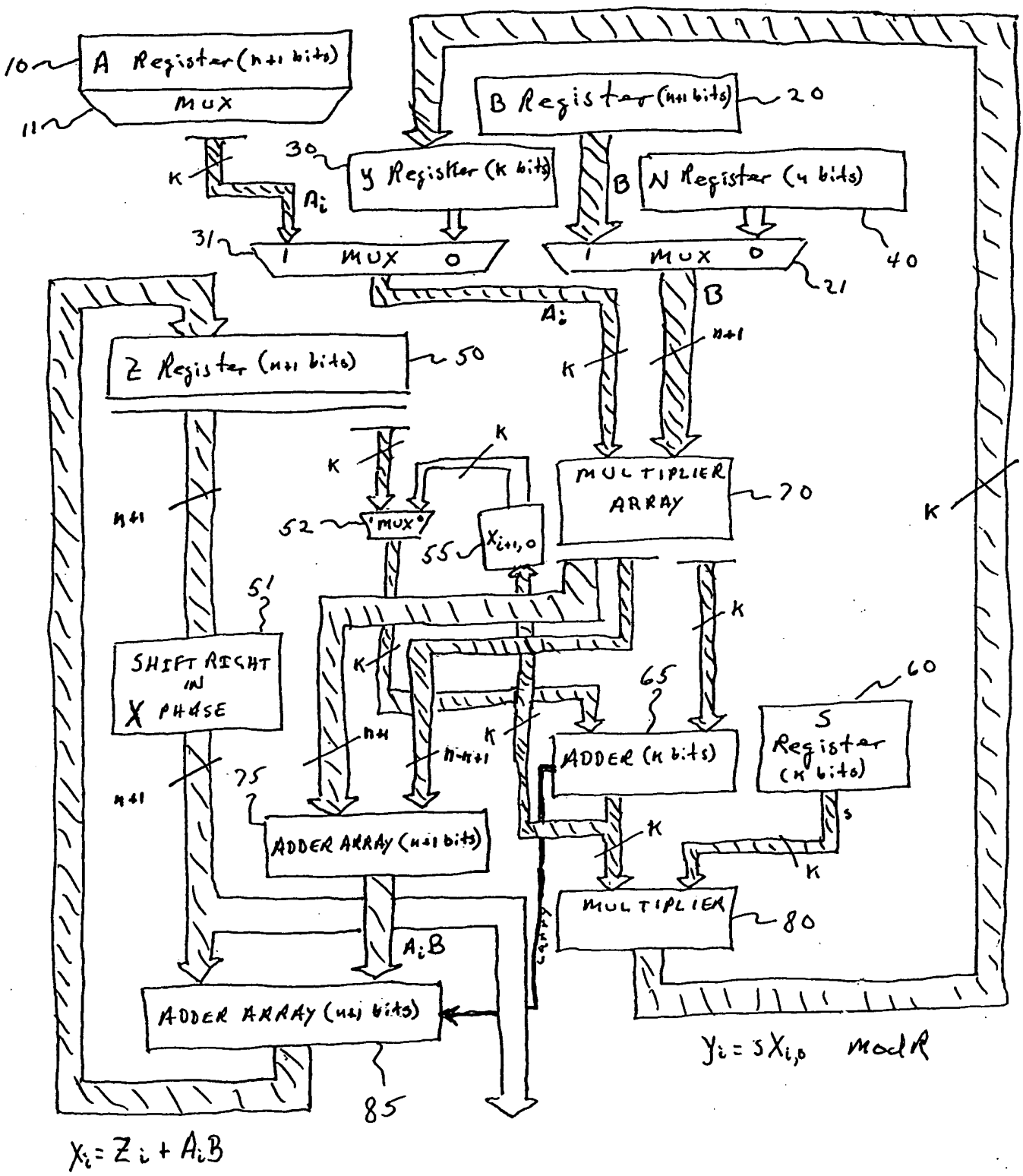
10
A Register (n+1 bits)
MUX
11
B Register (n+1 bits)
20
30
Y Register (K bits)
K
A_i
B
N Register (n bits)
31
1 MUX 0
1 MUX 0
40
21
A_i
B
Z Register (n+1 bits)
50
K
n+1
K
K
MULTIPLIER ARRAY
70
K
n+1
52
MUX
55
$X_{i+1,0}$
51
K
SHIFT RIGHT IN X PHASE
65
60
S Register (K bits)
n+1
75
n+1
n-n+1
K
ADDER (K bits)
ADDER ARRAY (n+1 bits)
K
K
MULTIPLIER
80
A_iB
ADDER ARRAY (n+1 bits)
85
$Y_i = SX_{i,0}$ mod R
$X_i = Z_i + A_iB$

Figure 2

POU920000124US1

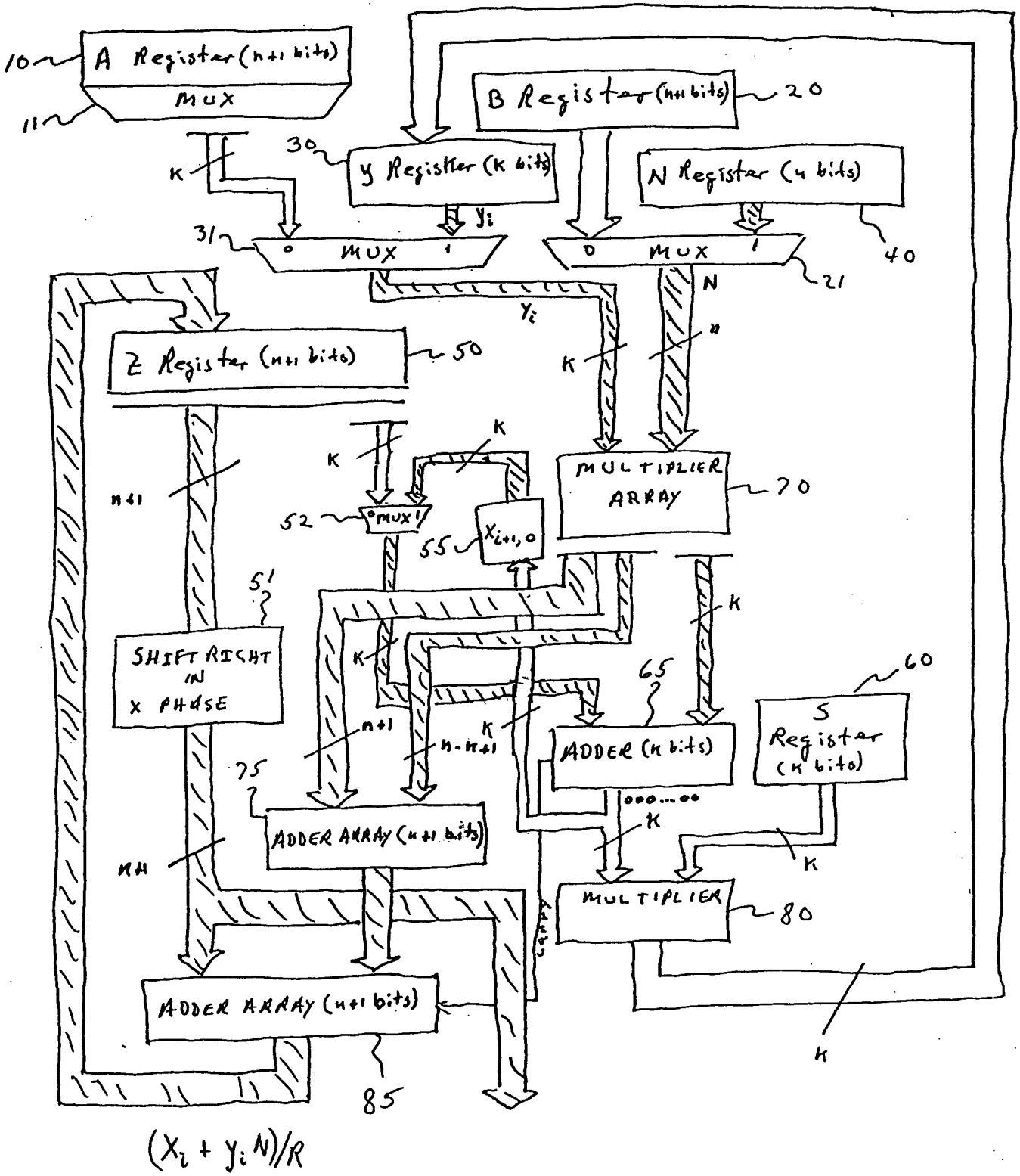

Figure 3

PCU92000 012451

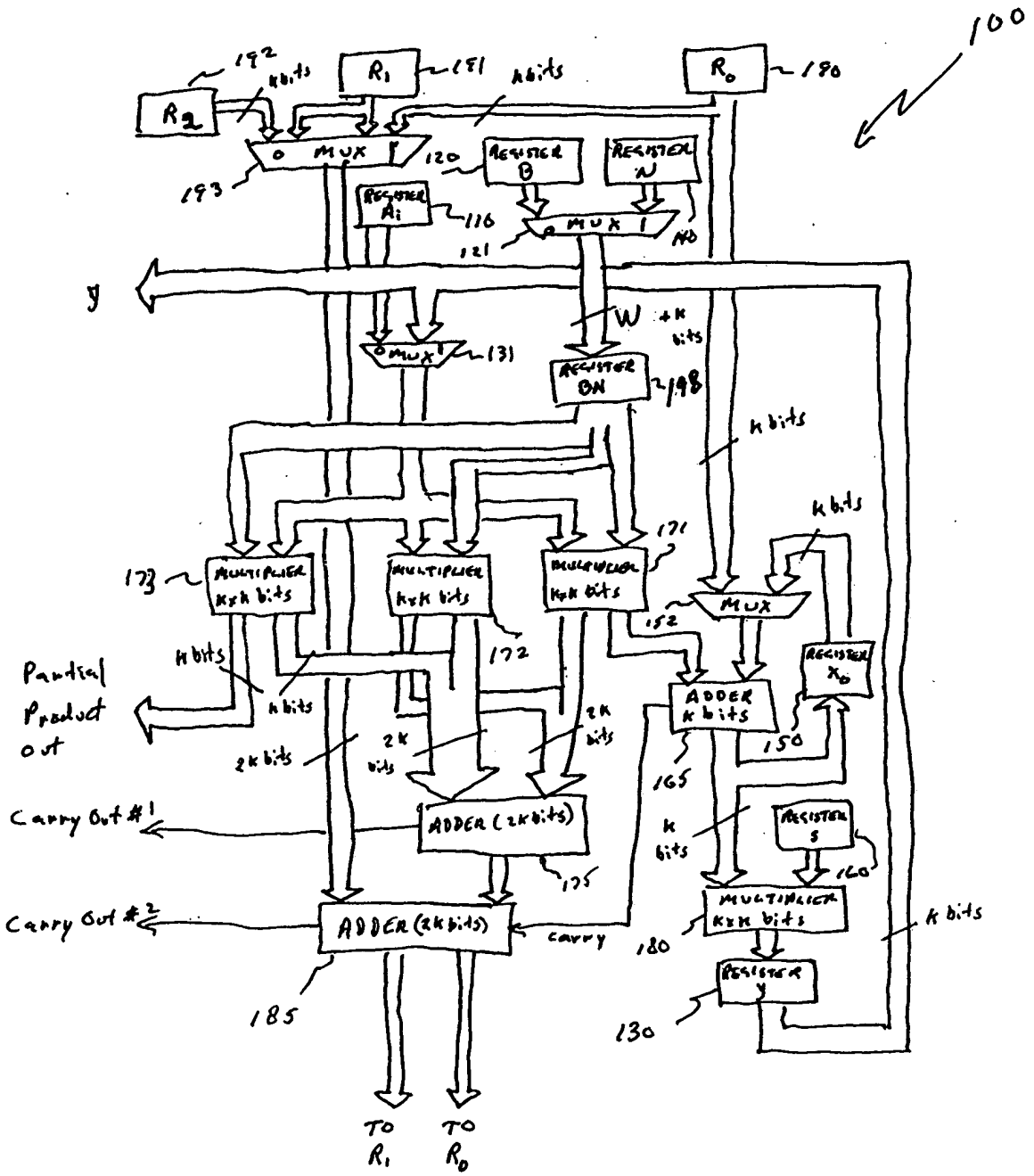

Figure 4

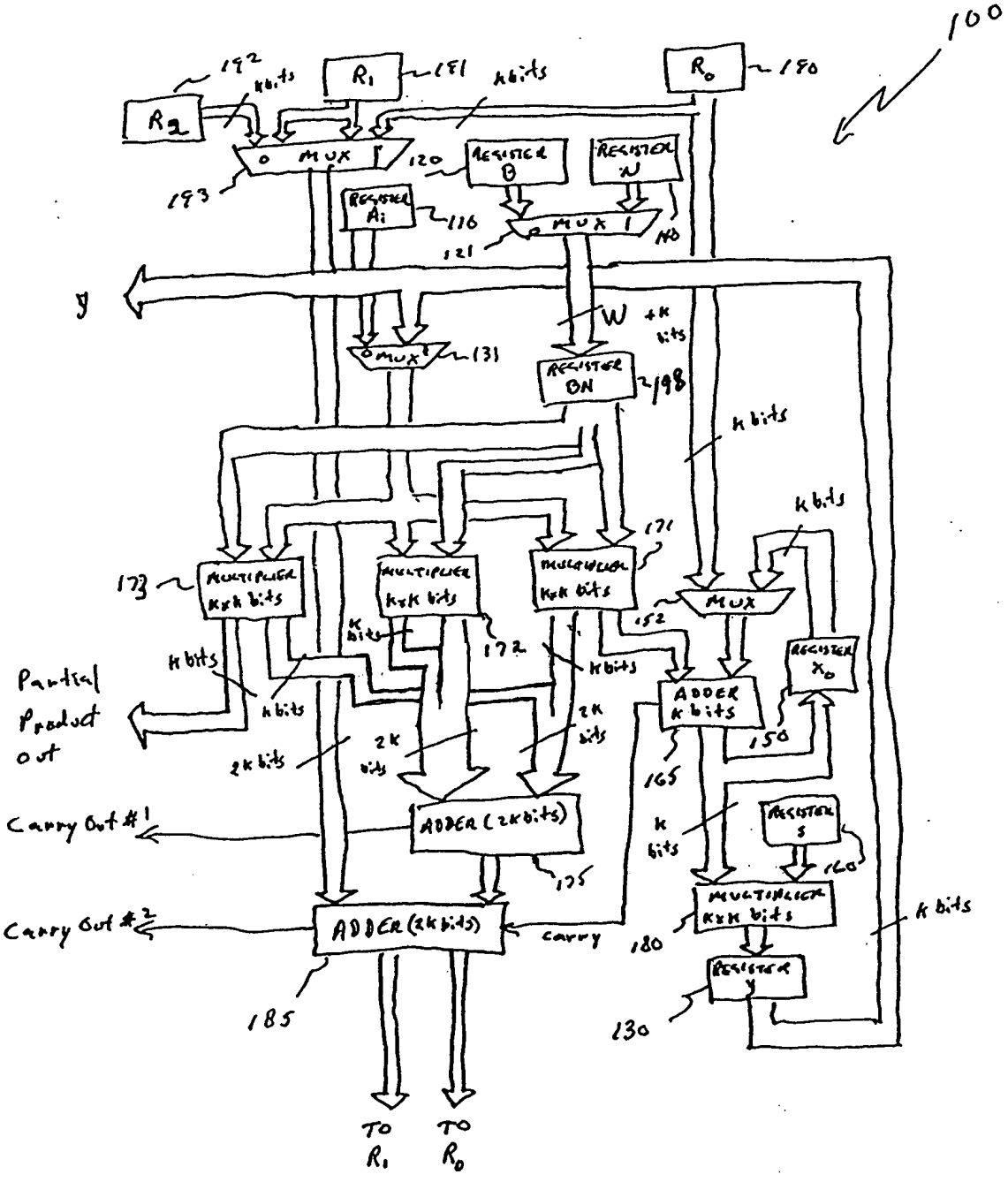
100
R2
192
k bits
R1
191
k bits
R0
190
MUX 0
193
120
REGISTER B
REGISTER N
REGISTER Ai
116
MUX 1
121
N0
y
W
2k bits
MUX 0
131
REGISTER ON
198
k bits
k bits
171
MULTIPLIER k x k bits
MULTIPLIER k x k bits
MULTIPLIER k x k bits
173
MUX
152
k bits
k bits
172
k bits
REGISTER X0
Partial Product out
k bits
k bits
ADDER k bits
150
2k bits
2k bits
2k bits
165
Carry Out #1
ADDER (2k bits)
k bits
REGISTER S
160
175
MULTIPLIER k x k bits
k bits
Carry Out #2
ADDER (2k bits)
carry
180
REGISTER Y
185
130
TO R1
TO R0

Figure 4A

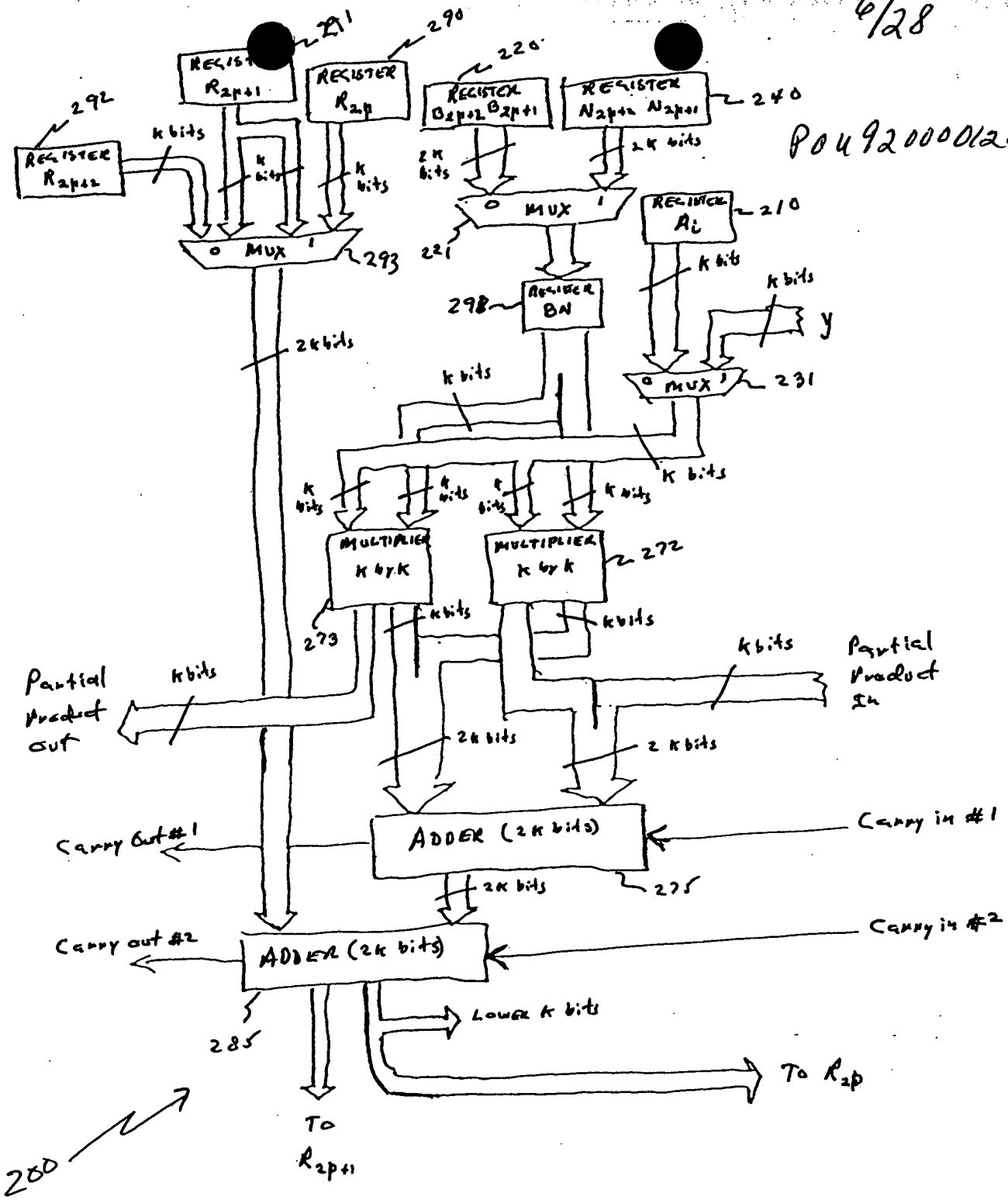
291
290
220
REGISTER R_{2p+1}
REGISTER R_{2p}
REGISTER $B_{2p+2}B_{2p+1}$
REGISTER $N_{2p+2}N_{2p+1}$
240
292
REGISTER R_{2p+2}
k bits
2k bits
MUX
221
293
REGISTER A_i
210
298
REGISTER BN
y
231
MULTIPLIER k by k
272
273
Partial Product out
Partial Product In
ADDER (2k bits)
Carry Out #1
Carry in #1
275
Carry out #2
Carry in #2
285
Lower k bits
To R_{2p}
To R_{2p+1}
200

Figure 5

POU920000124US1

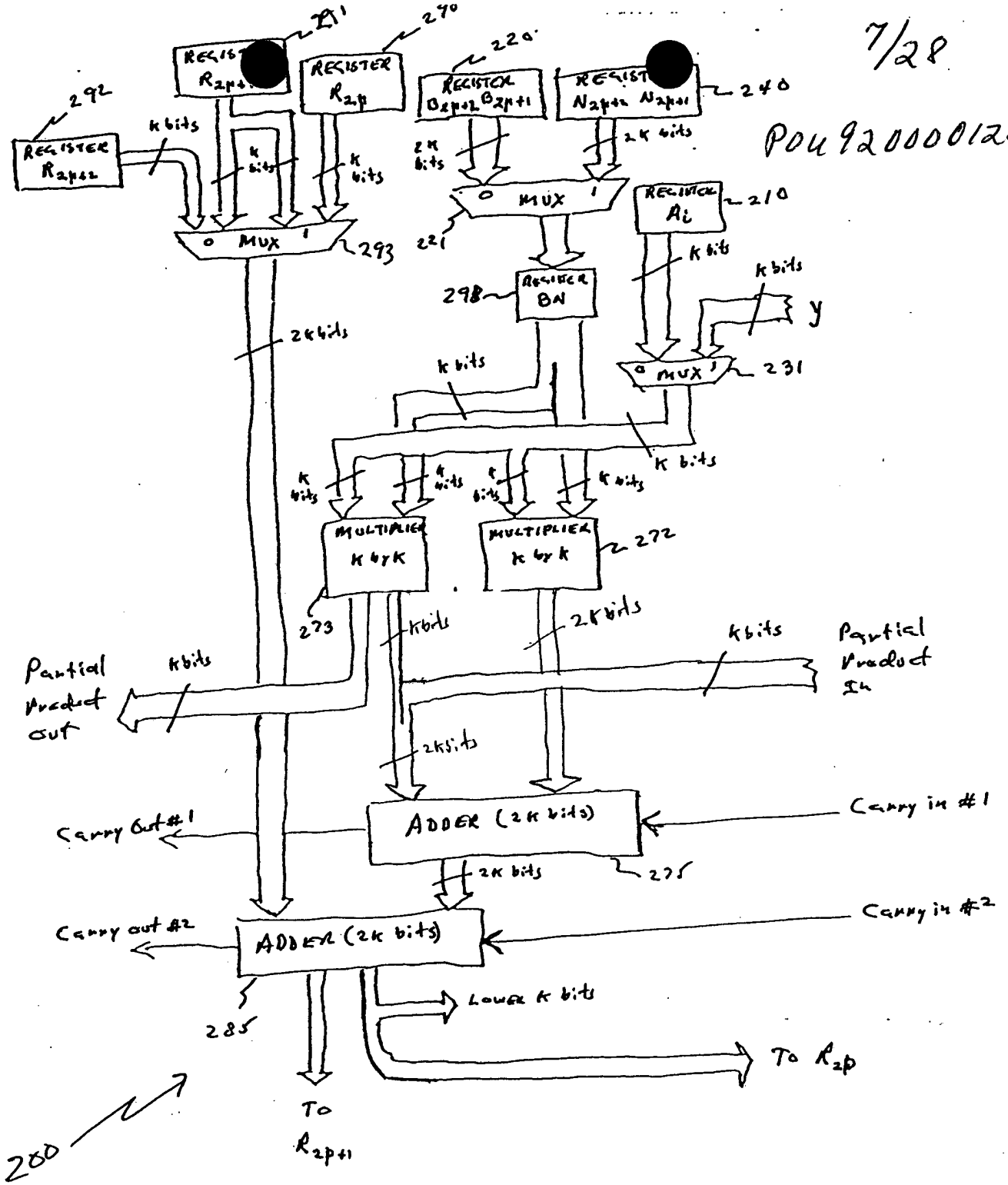

Figure 5A

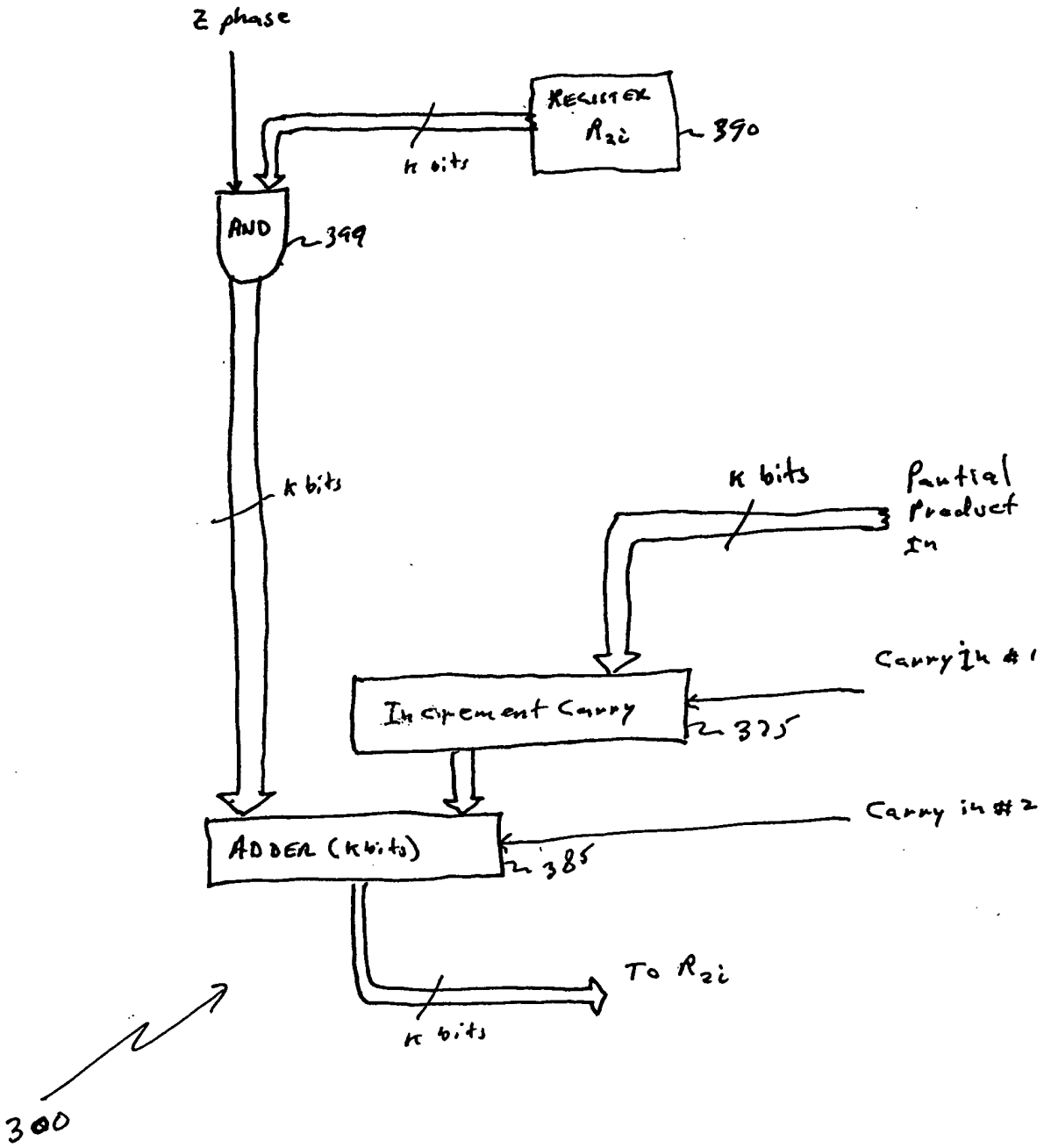
Z phase
REGISTER
R_{zi}
390
K bits
AND
399
K bits
K bits
Partial
Product
In
Carry In #1
Increment Carry
395
Carry in #2
ADDER (K bits)
385
To R_{zi}
K bits
300

Figure 6

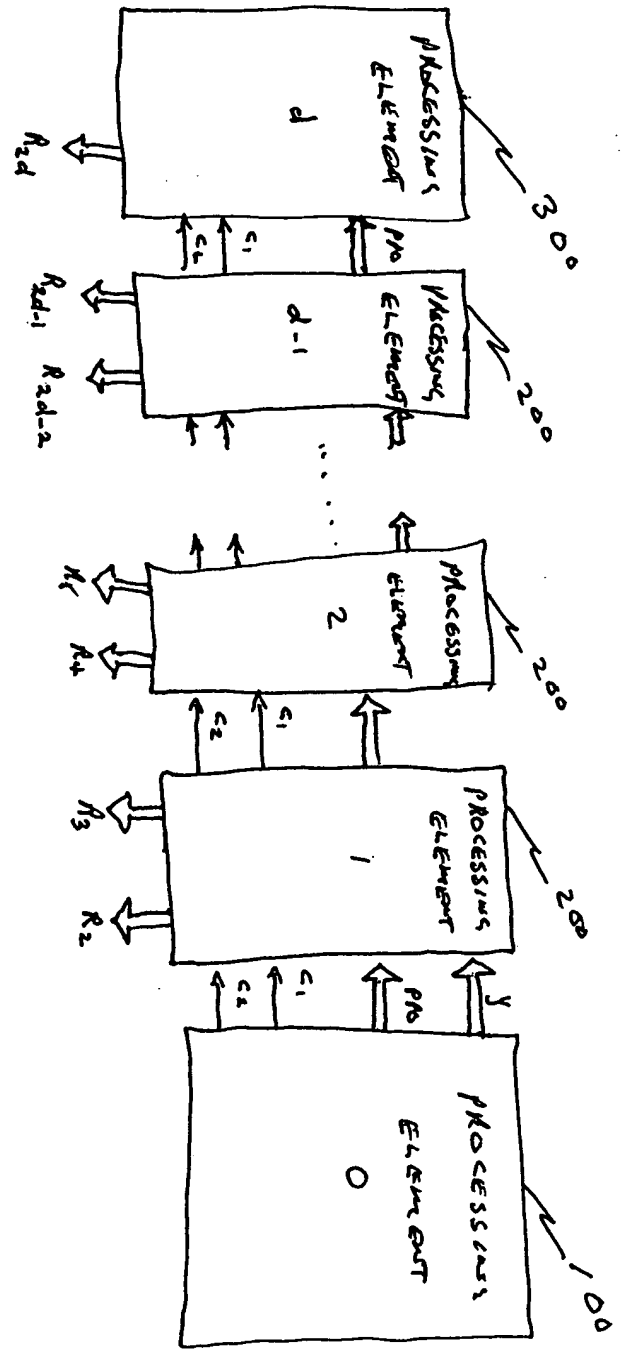
PROCESSING ELEMENT
d
300
R_{2d}
C_2
C_1
P/D
PROCESSING ELEMENT
d-1
200
R_{2d-1}
R_{2d-2}
PROCESSING ELEMENT
2
200
R_1
R_4
PROCESSING ELEMENT
1
200
R_3
R_2
Y
PROCESSING ELEMENT
0
100

Figure 7

PQU92000 0124481

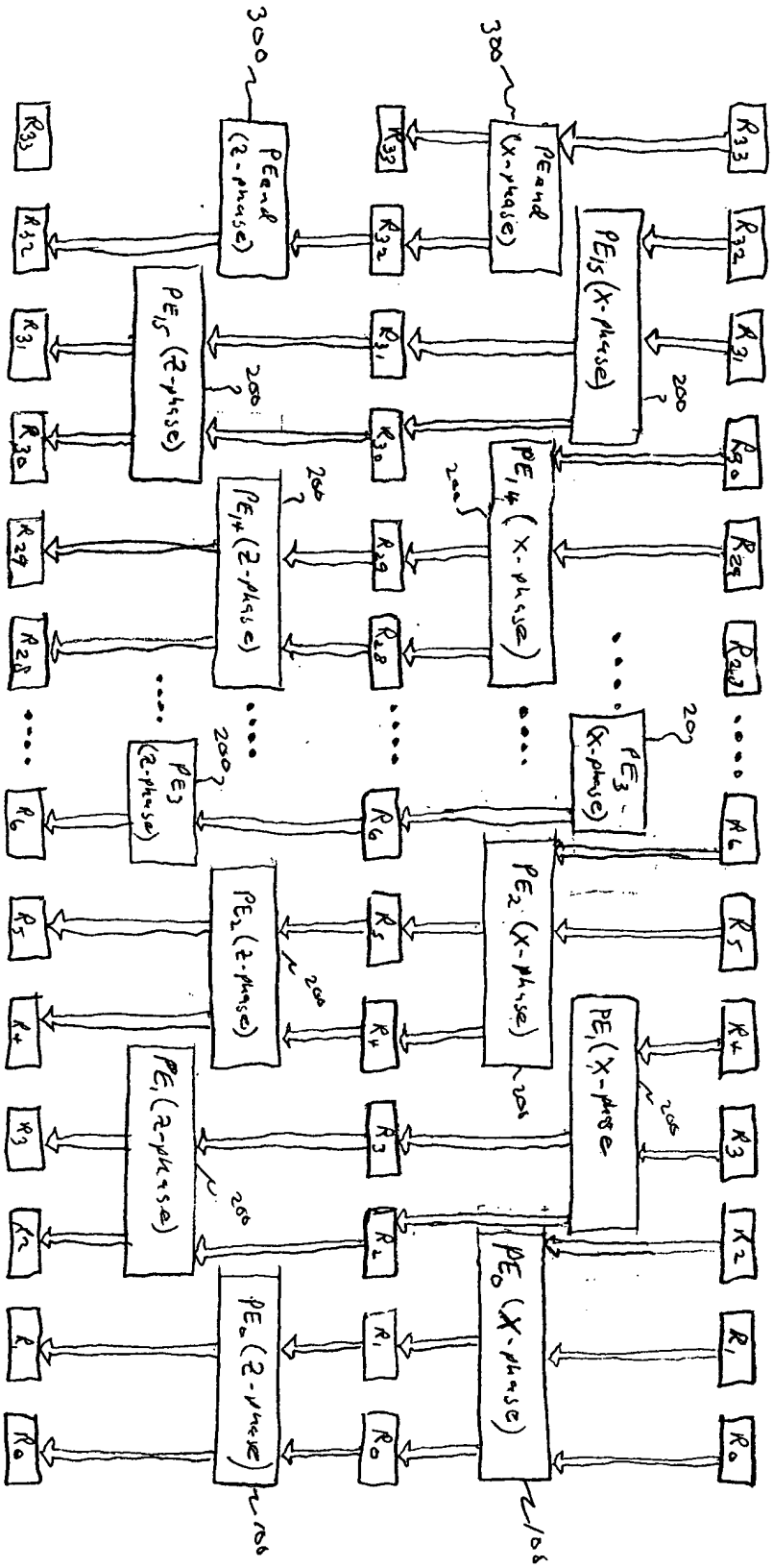

Figure 8

PCU92000124US1

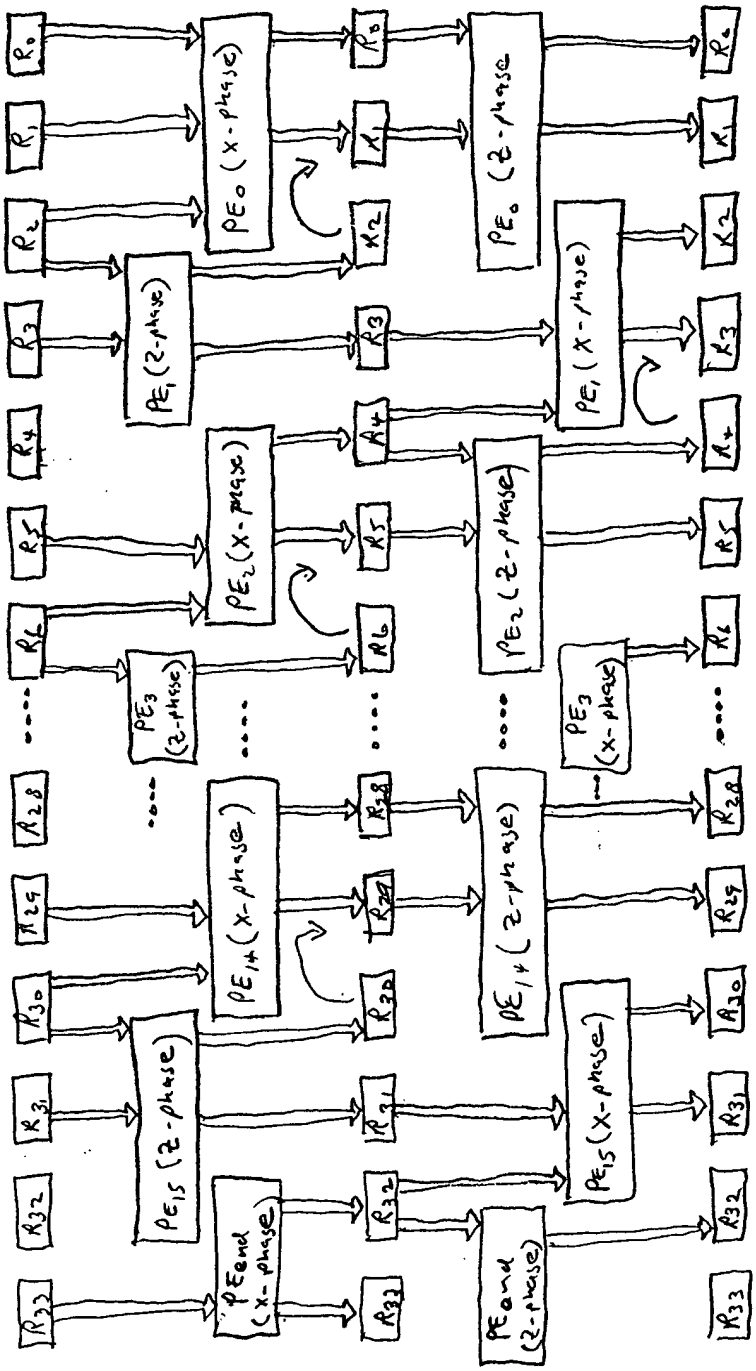

Figure 9

POU920000124US1

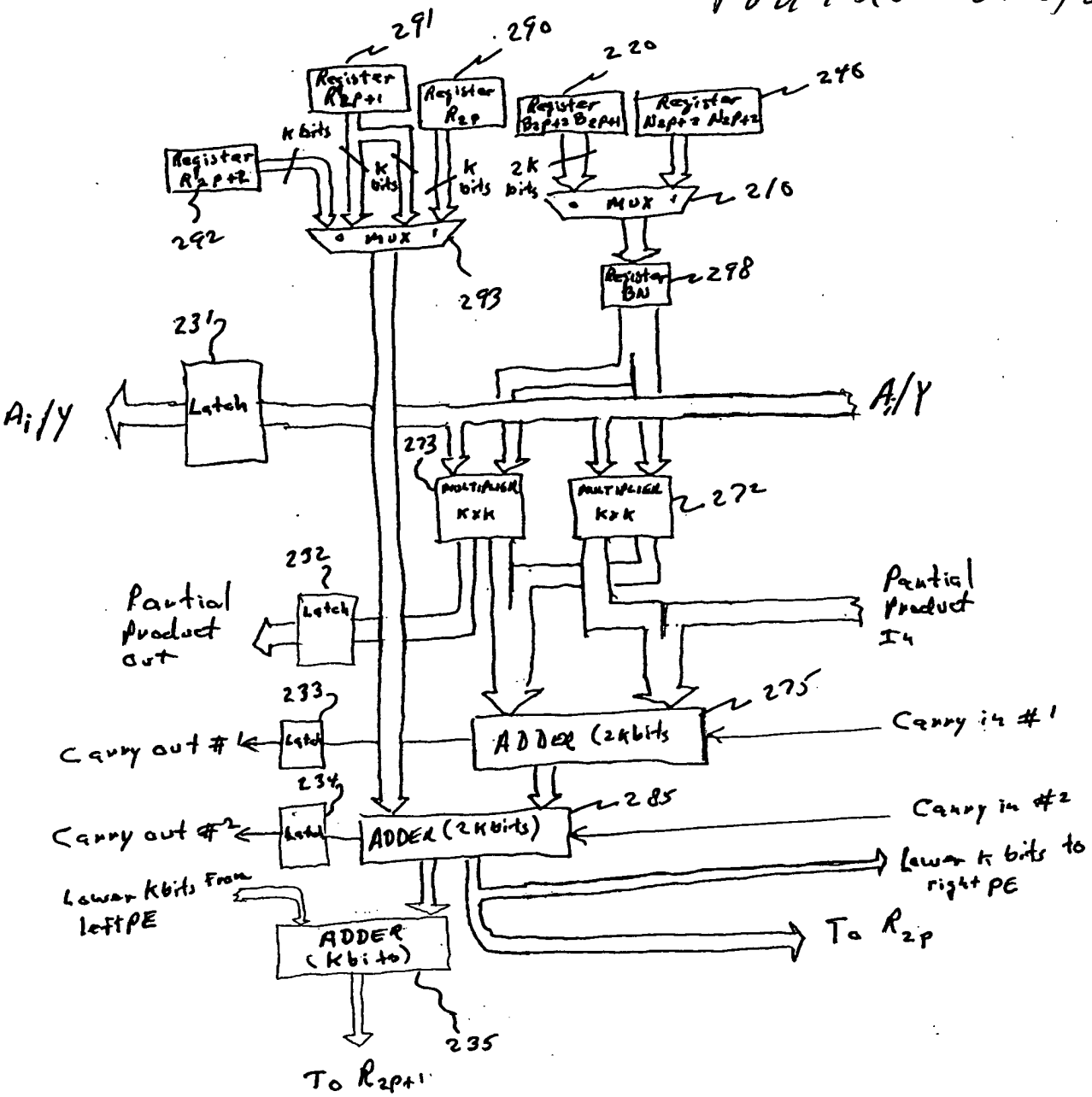

Figure 10

PD4920000124US1

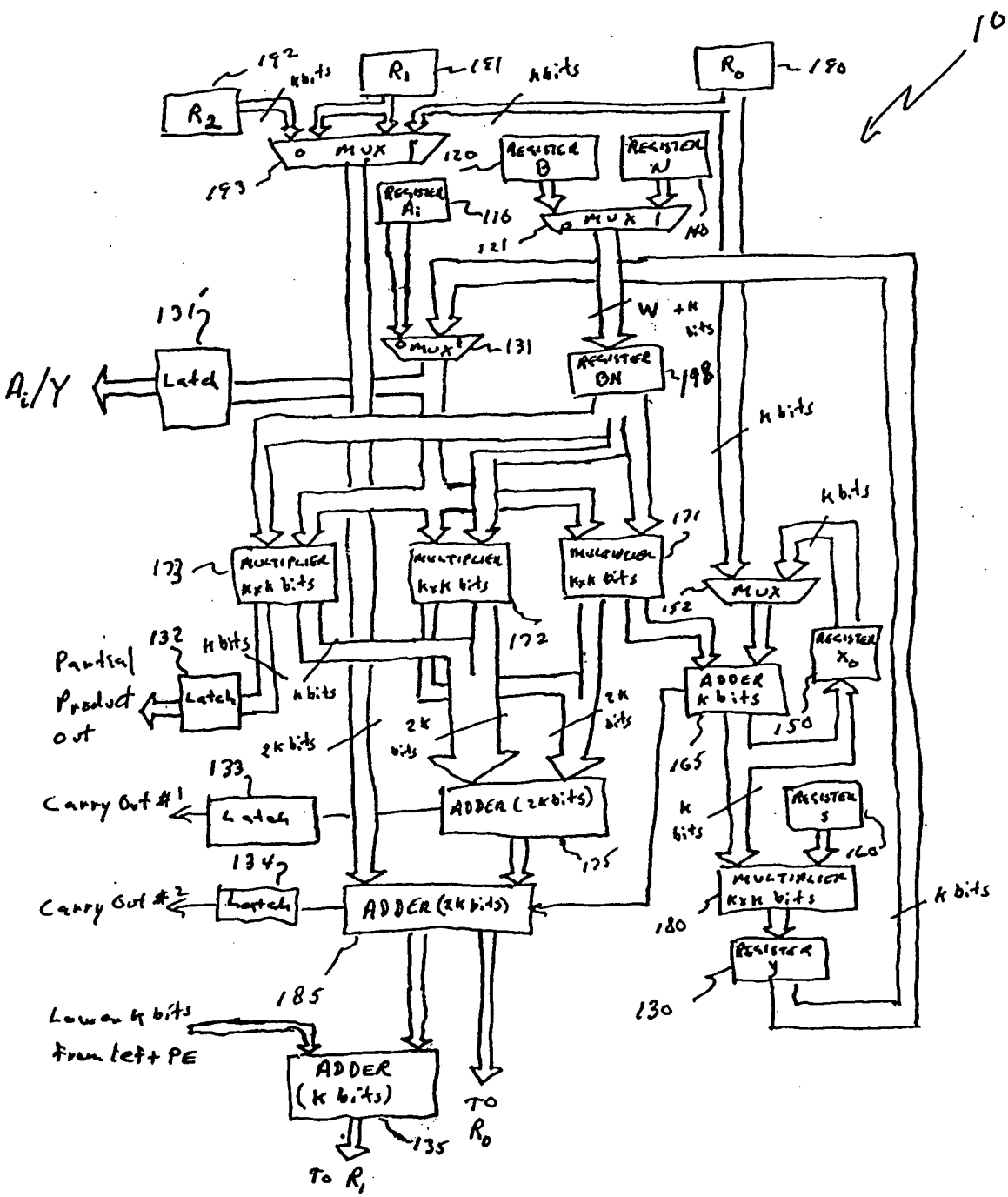

Figure 11

POU92000 0124US1

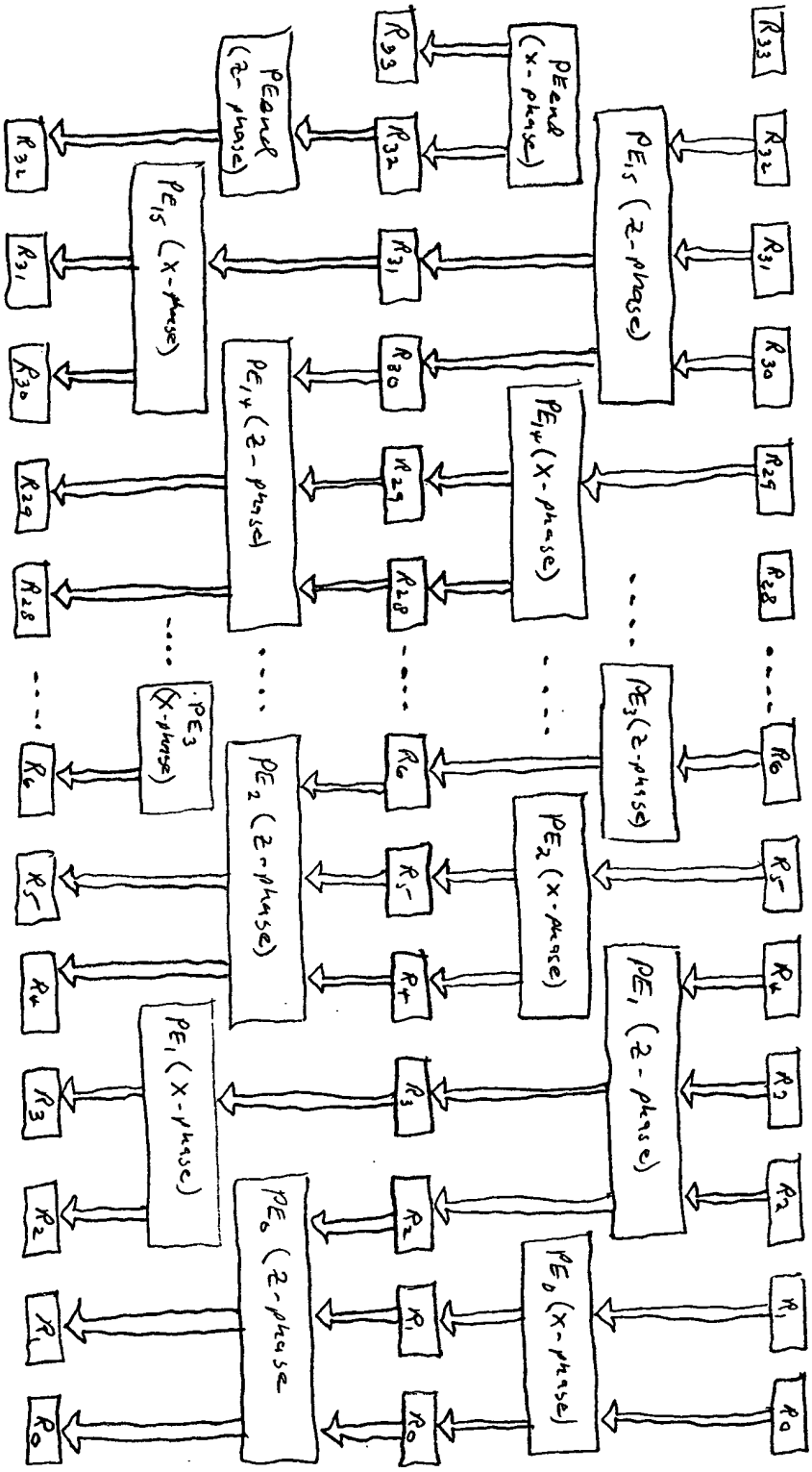

Figure 12

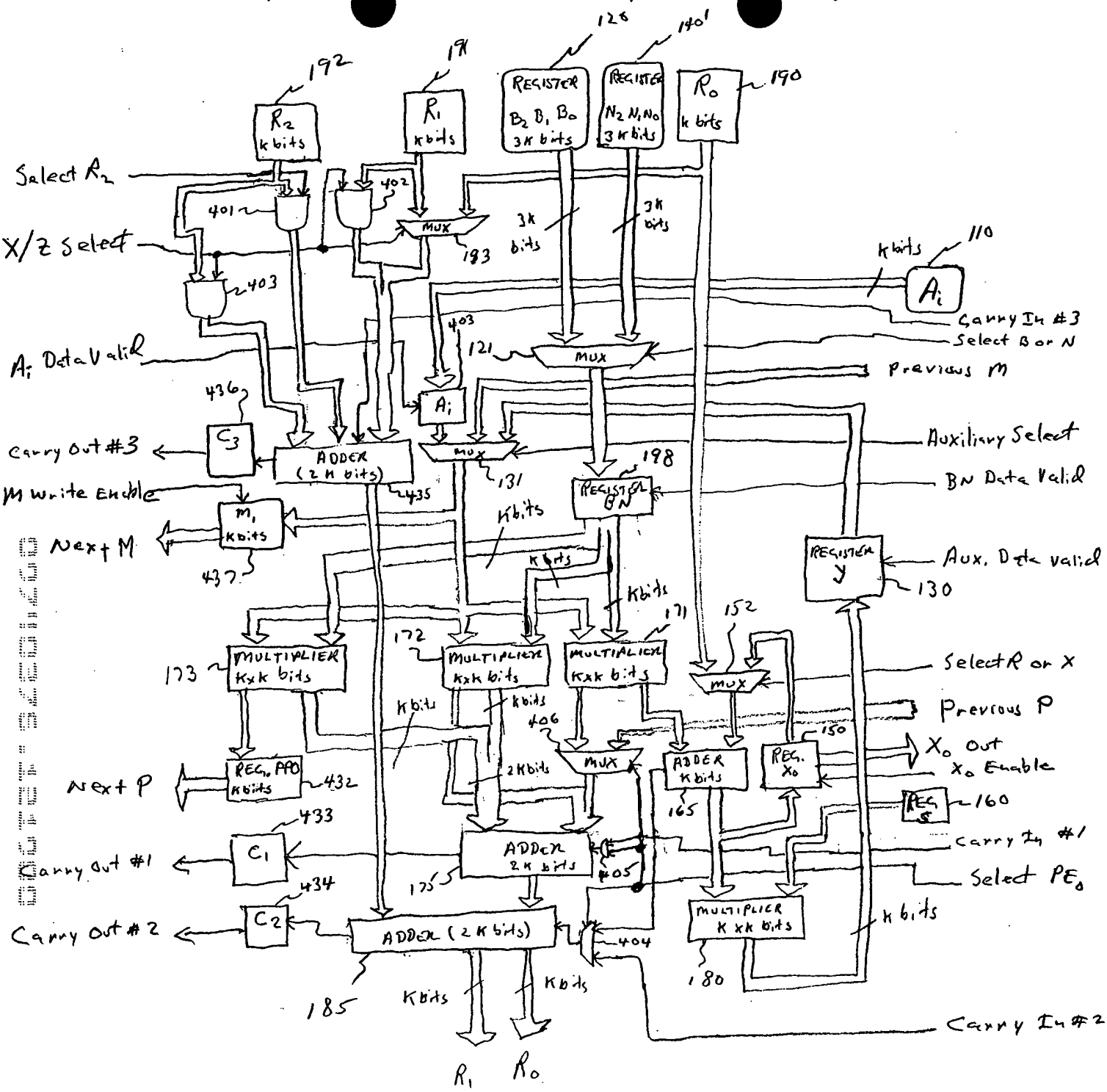
192
191
125'
140'
190
R_2 k bits
R_1 k bits
REGISTER B_2 B_1 B_0 3K bits
REGISTER N_2 N_1 N_0 3K bits
R_0 k bits
Select R_2
401
402
MUX
193
3K bits
3K bits
X/Z Select
403
110
k bits
A_i
Carry In #3
Select B or N
A_i Data Valid
403
121
MUX
Previous M
436
A_i
Auxiliary Select
Carry out #3
C_3
ADDER (2K bits)
MUX
131
198
REGISTER BN
BN Data Valid
M write Enable
M_1 Kbits
435
Kbits
Next M
437
Kbits
REGISTER Y
Aux. Data valid
130
Kbits
171
152
172
MULTIPLIER KxK bits
MULTIPLIER KxK bits
MULTIPLIER KxK bits
MUX
Select R or X
173
Kbits
Kbits
Previous P
406
150
MUX
ADDER K bits
REG. X_0
X_0 out
X_0 Enable
REG. PP0 Kbits
2Kbits
165
REG. S
160
Next P
432
433
C_1
ADDER 2K bits
Carry In #1
Carry out #1
405
175
Select PE_0
434
C_2
MULTIPLIER K xK bits
K bits
Carry out #2
ADDER (2K bits)
404
180
185
Kbits
Kbits
Carry In #2
R_1
R_0

Figure 13

PO4920000124481

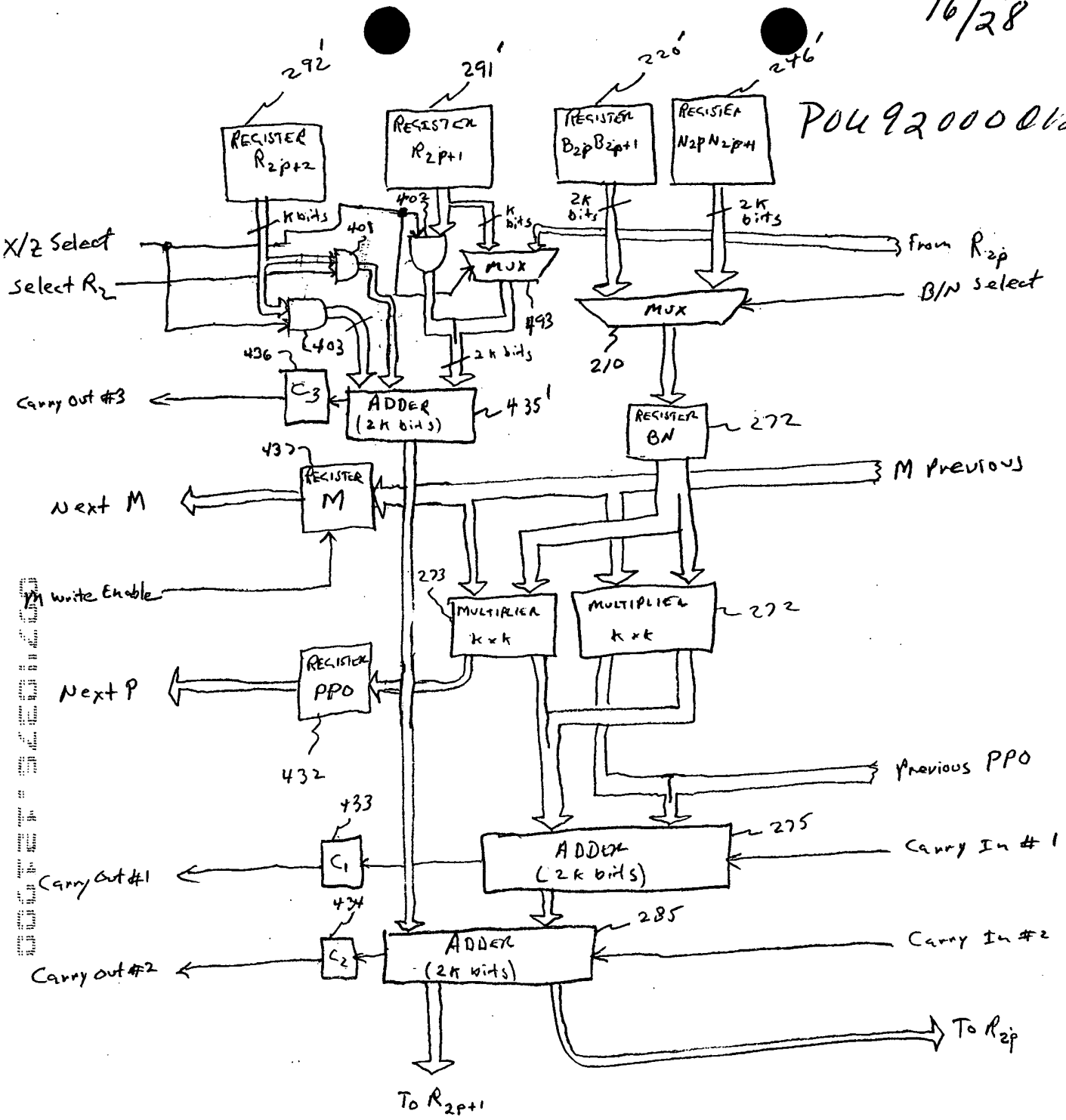

Figure 14

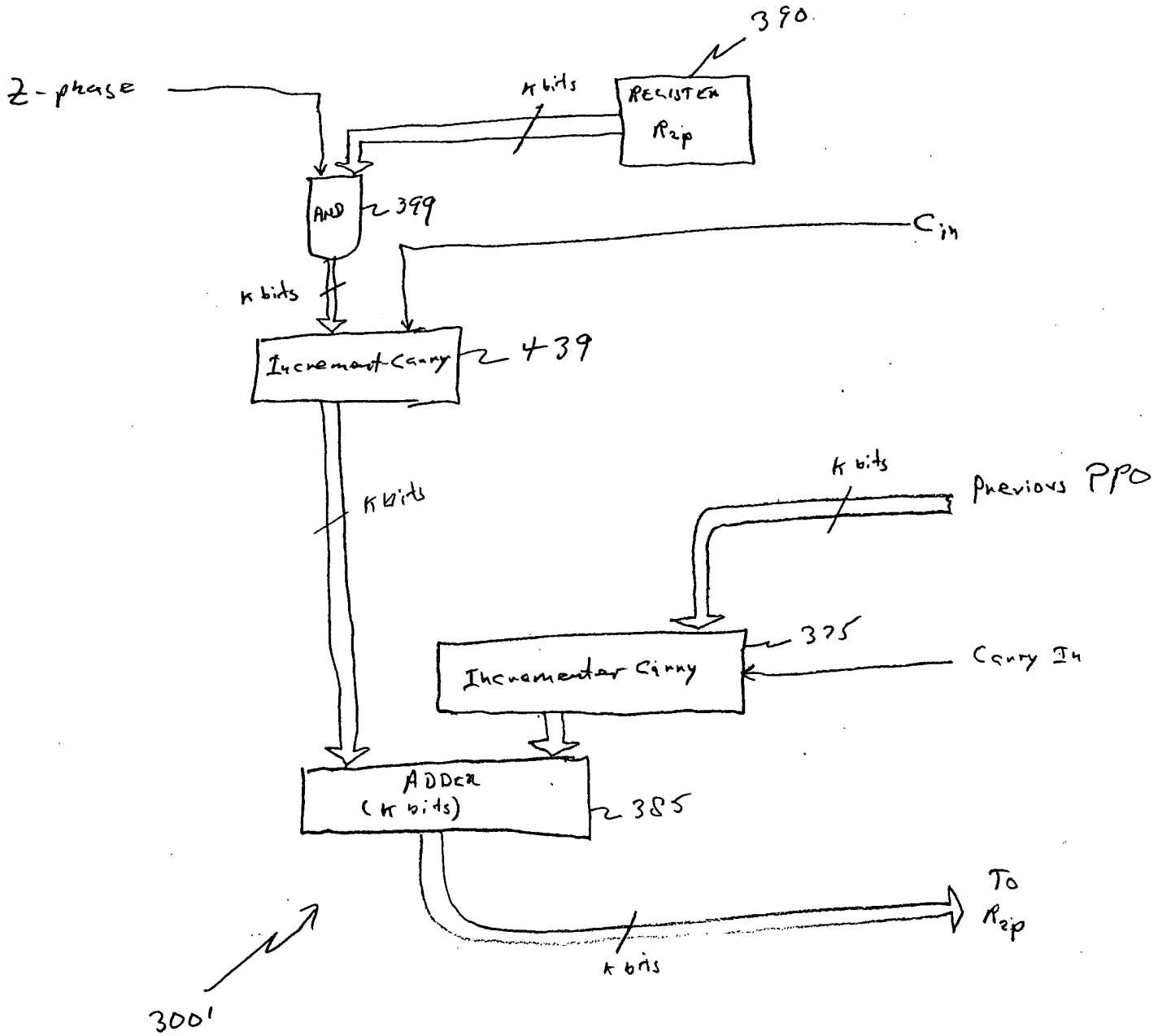
390
Z-phase
K bits
REGISTER
R_{zp}
AND
399
C_{in}
K bits
Increment-Carry
439
K bits
K bits
Previous PPO
Incrementer Carry
375
Carry In
ADDER
(K bits)
385
To
R_{zp}
K bits
300'

Figure 15

P0492000012445S1

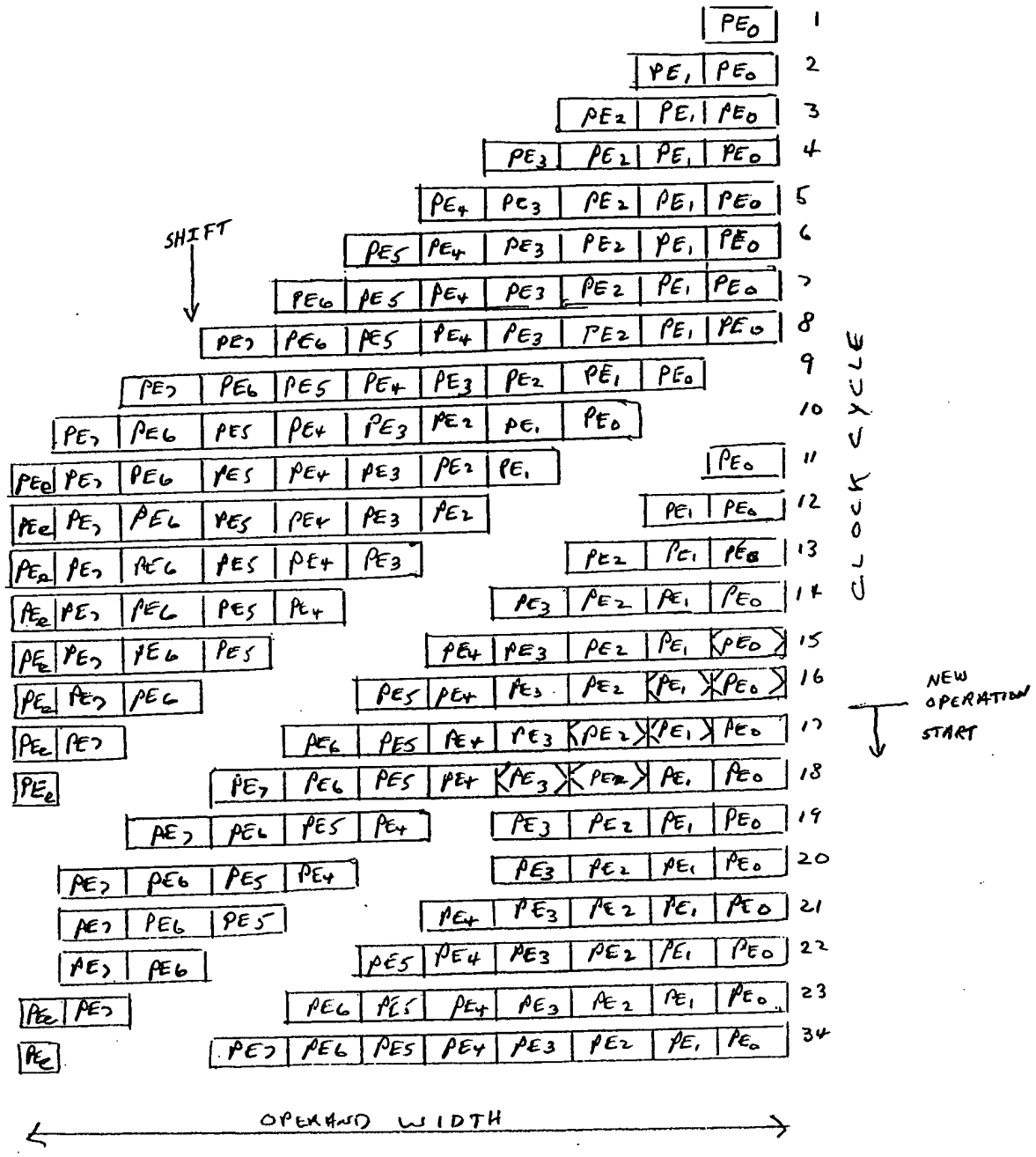

Figure 16

PU920000124US1

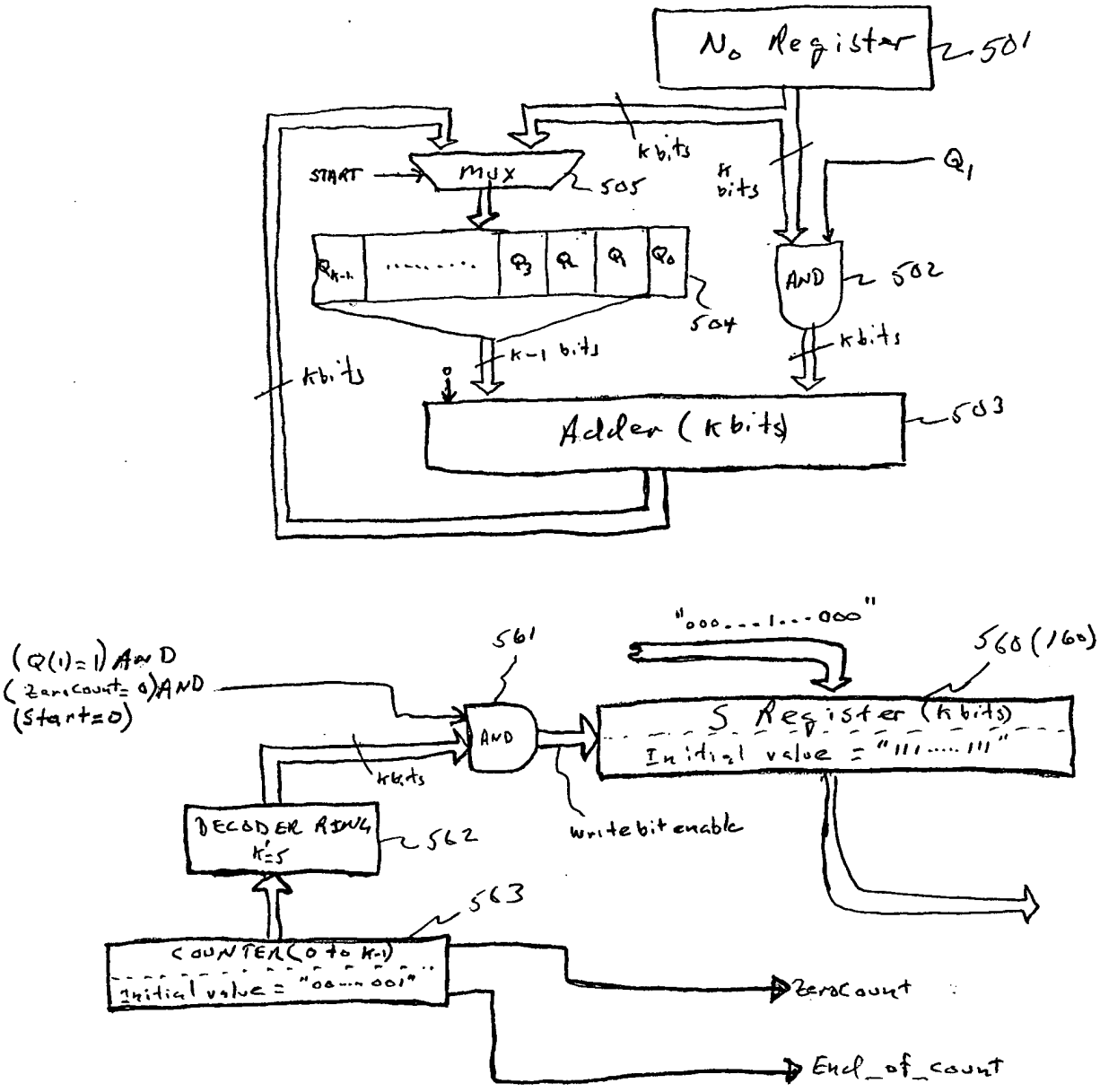

Figure 17

P04920000124US1

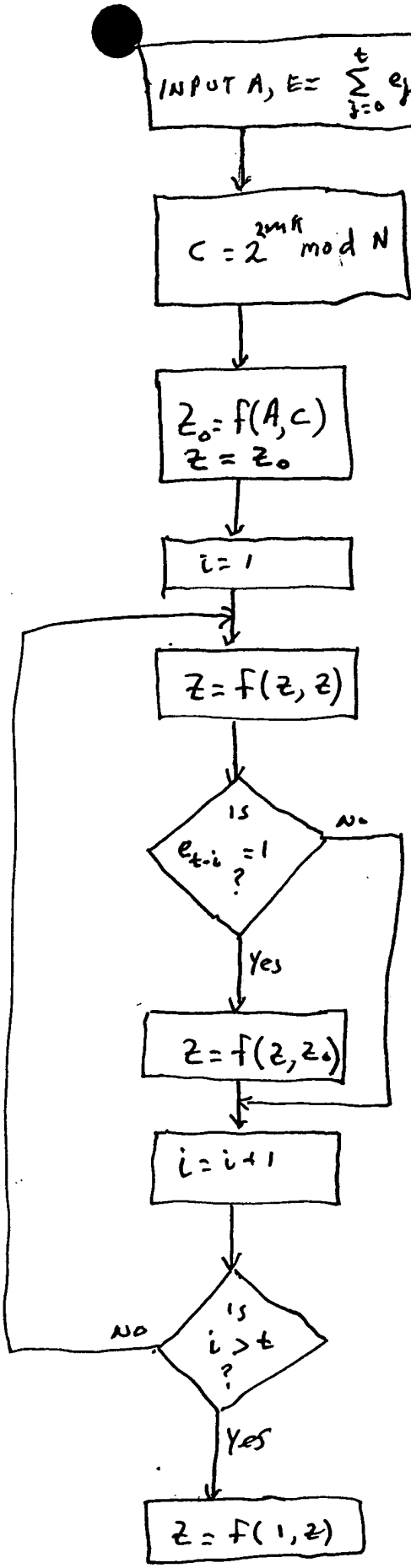

Figure 18

PO4920000124451

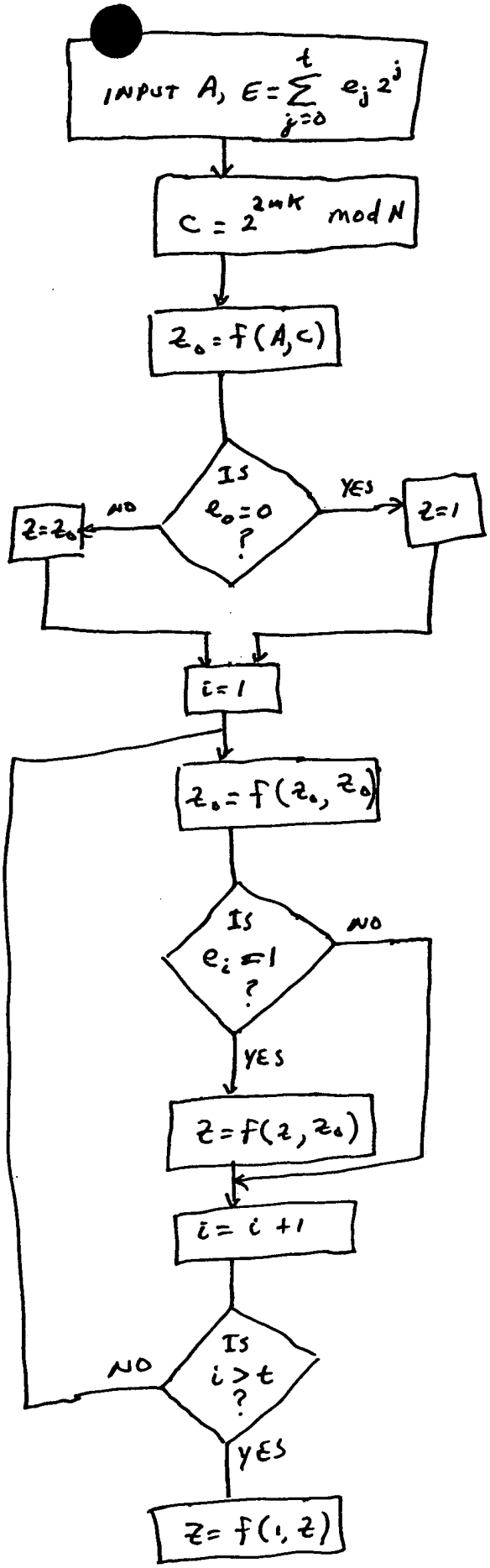

Figure 19

EP 0492000 A1 124451

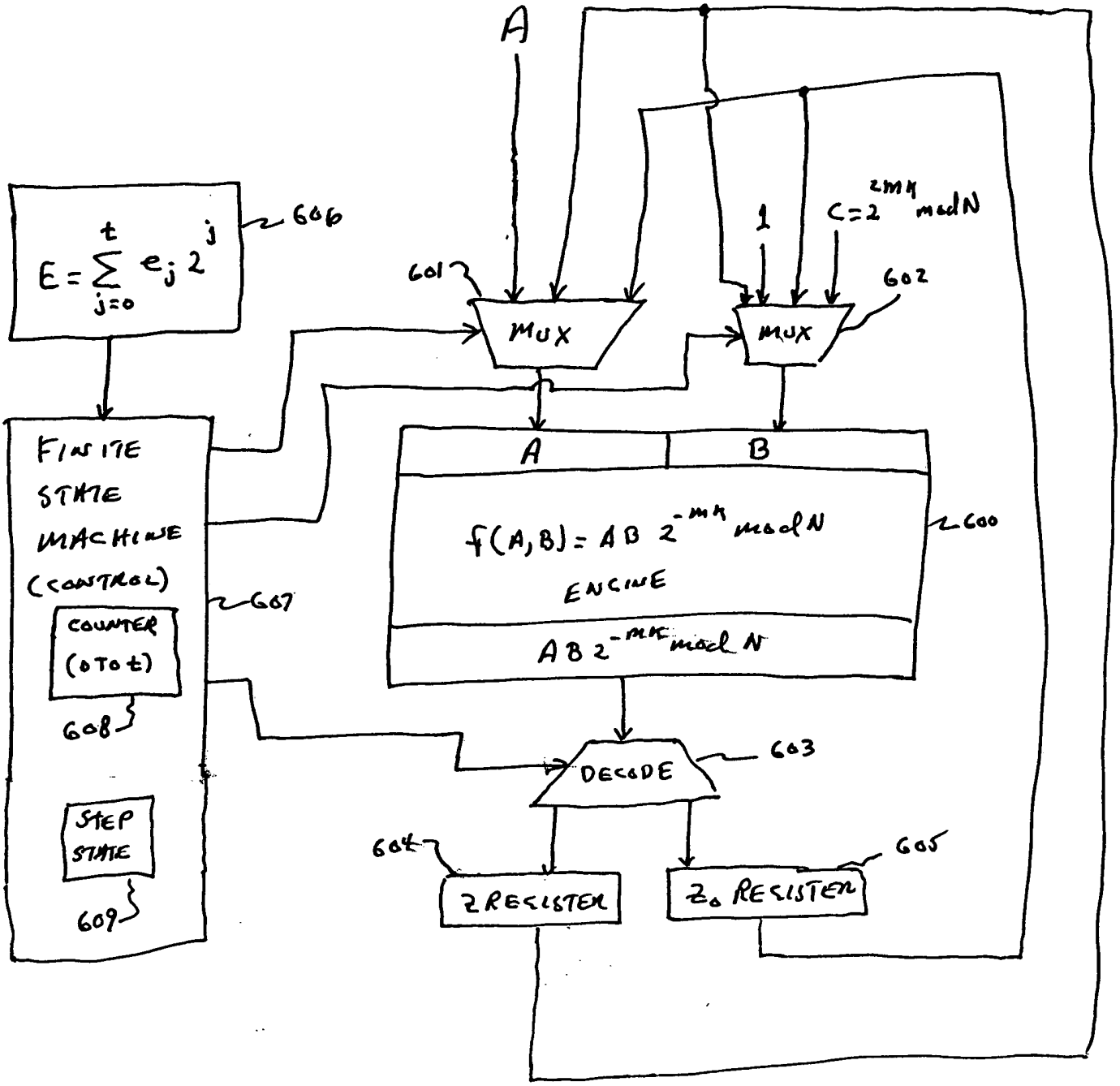

Figure 20

92000 0124451

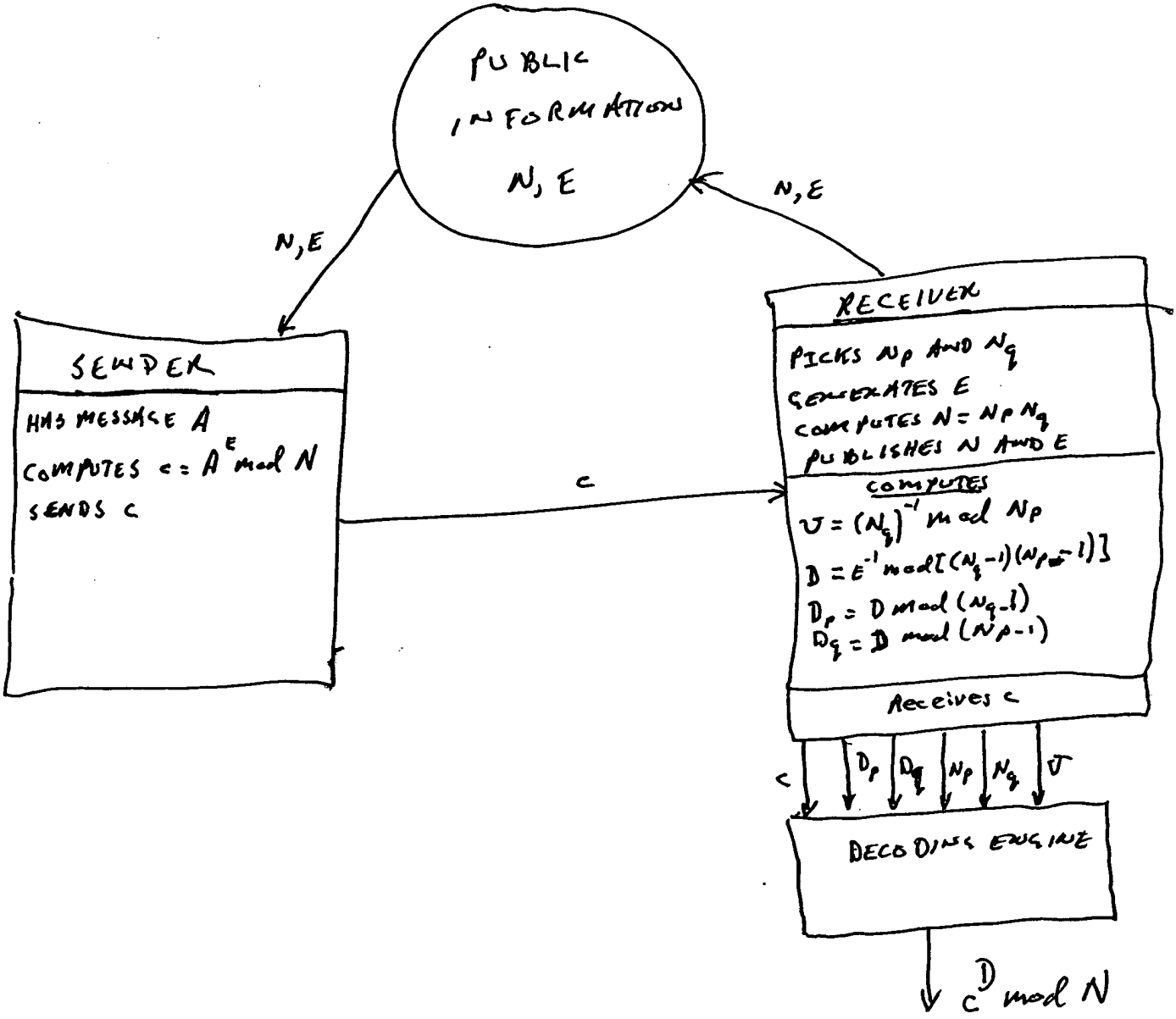

Figure 21

FR920000124US1

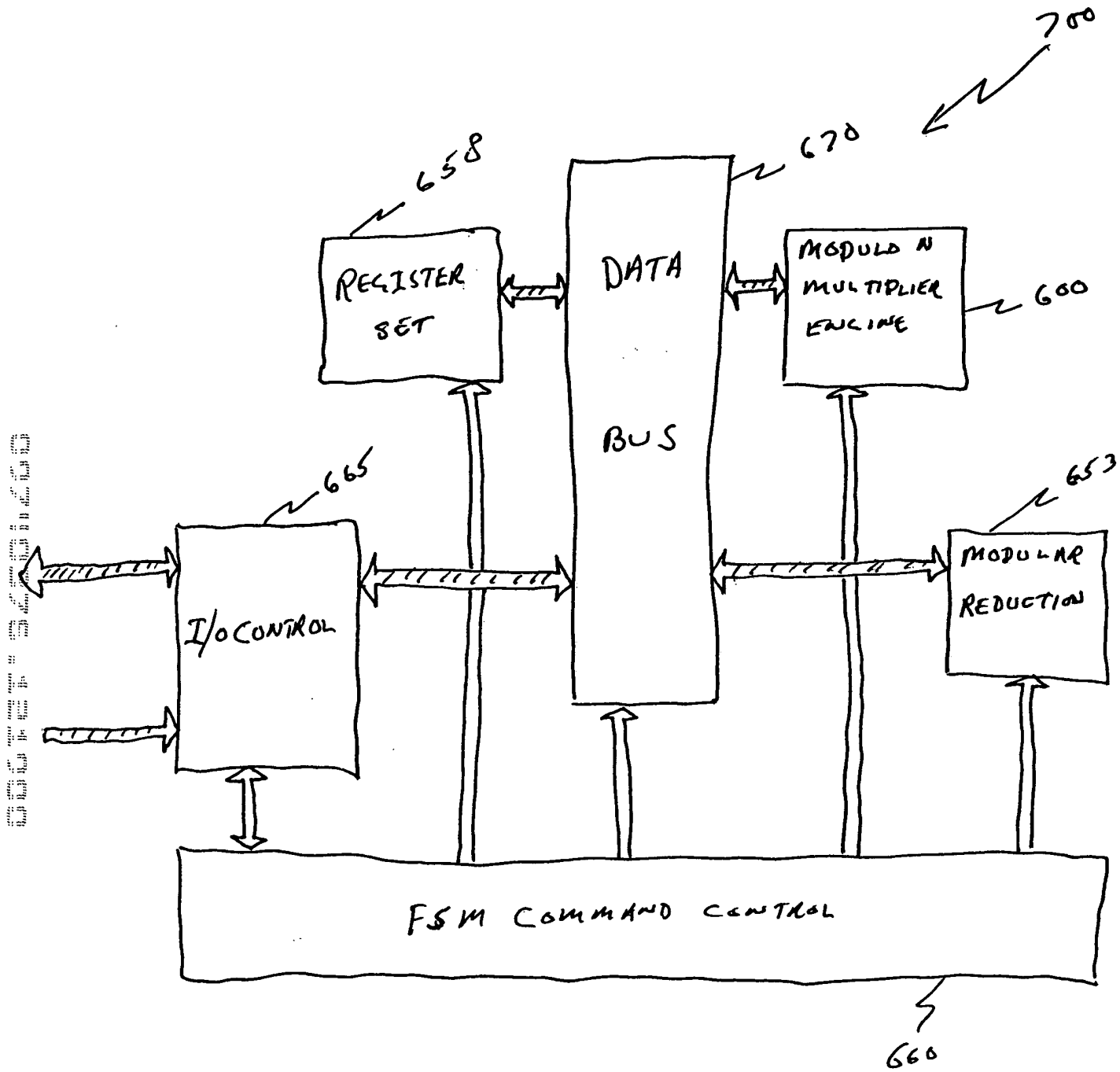

Figure 22

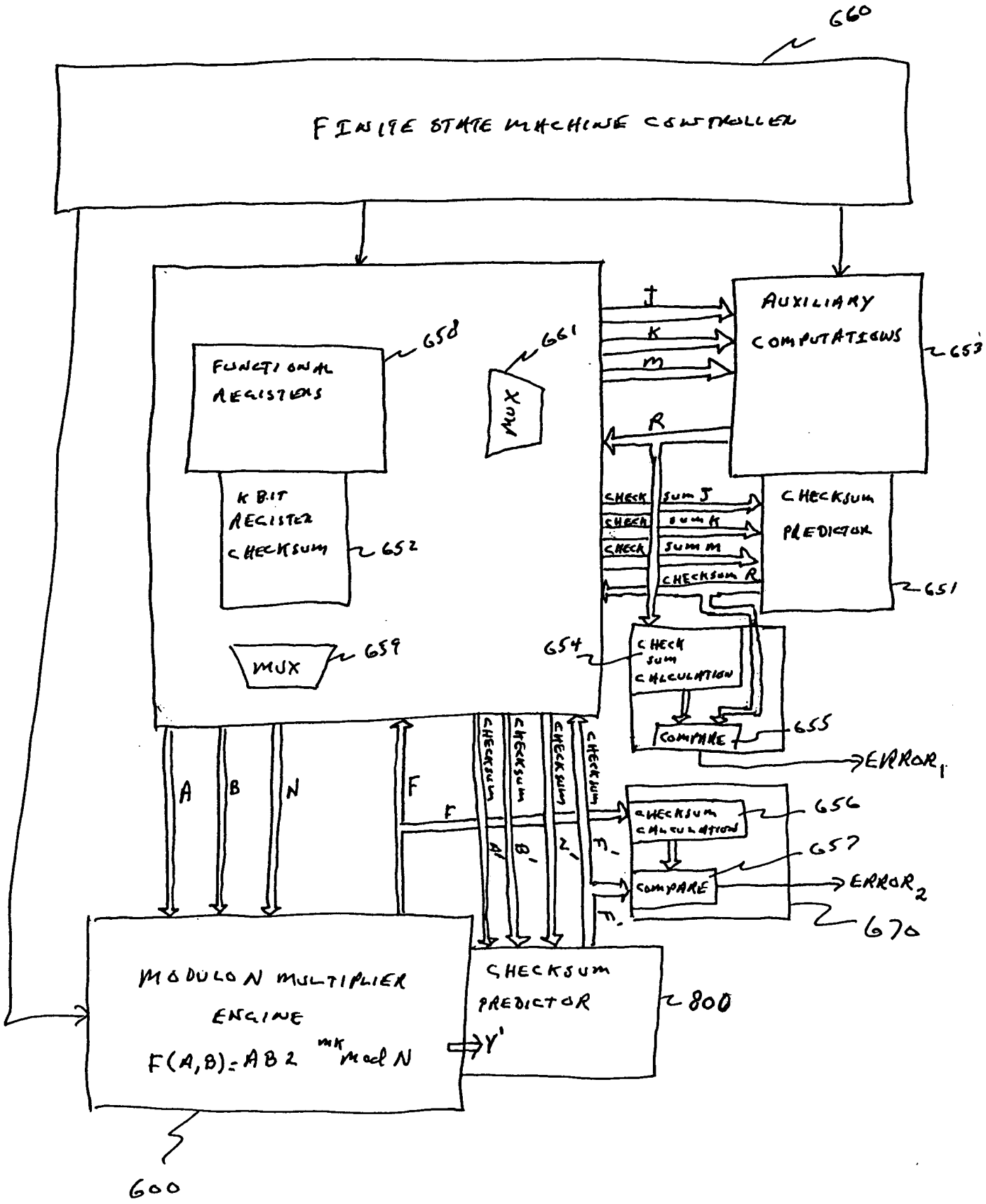
660
FINITE STATE MACHINE CONTROLLER
FUNCTIONAL REGISTERS
658
661
MUX
K BIT REGISTER CHECKSUM
652
MUX
659
654
J
K
M
R
AUXILIARY COMPUTATIONS
653
CHECK SUM J
CHECK SUM K
CHECK SUM M
CHECKSUM R
CHECKSUM PREDICTOR
651
CHECK SUM CALCULATION
COMPARE
655
ERROR1
A
B
N
F
F
CHECKSUM
CHECKSUM
CHECKSUM
CHECKSUM
A'
B'
Z'
F'
F'
CHECKSUM CALCULATION
656
657
COMPARE
ERROR2
670
MODULO N MULTIPLIER ENGINE
F(A,B) = AB2^MK mod N
CHECKSUM PREDICTOR
800
Y'
600

Figure 23

POU920000124US1

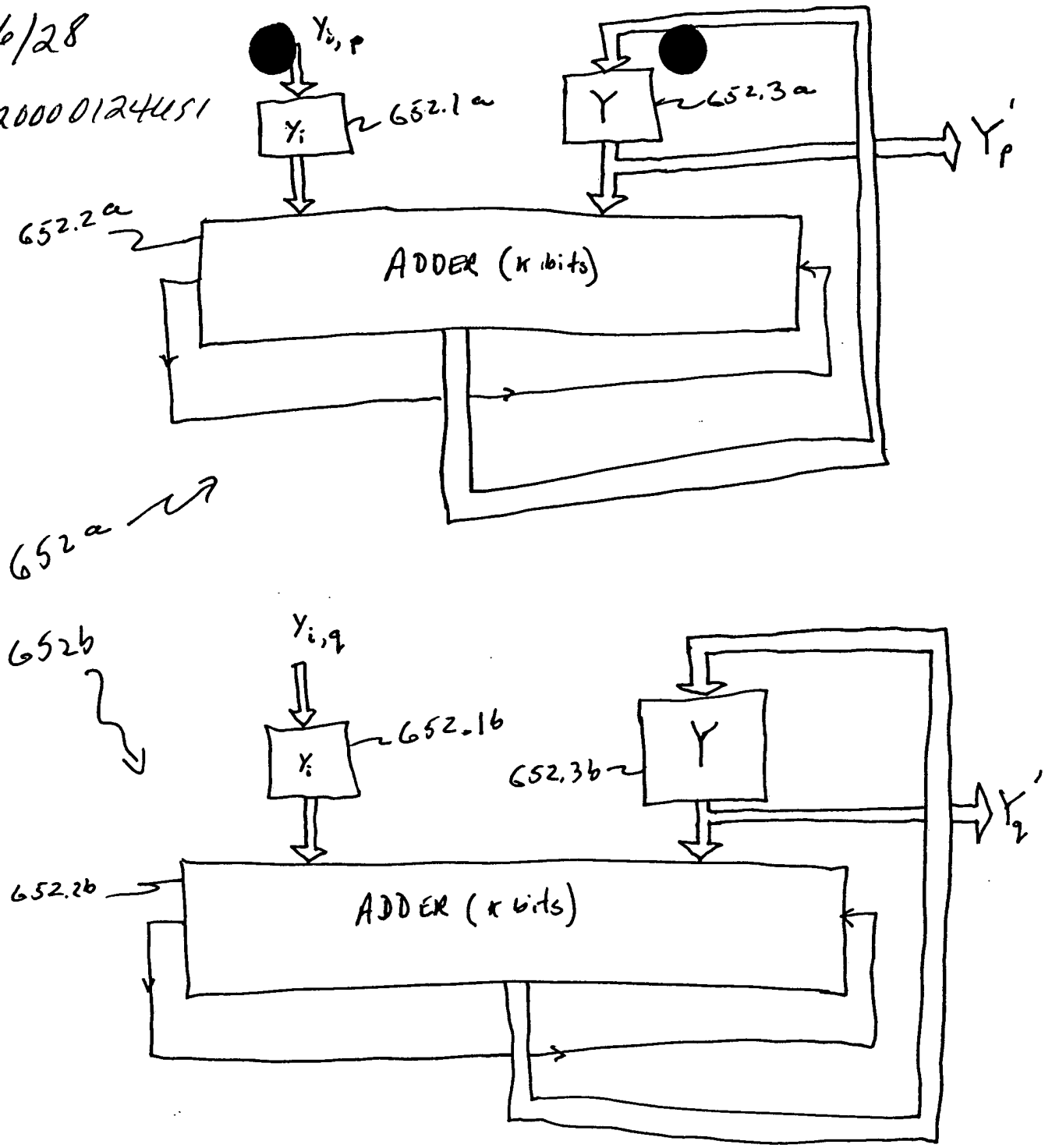

Figure 24

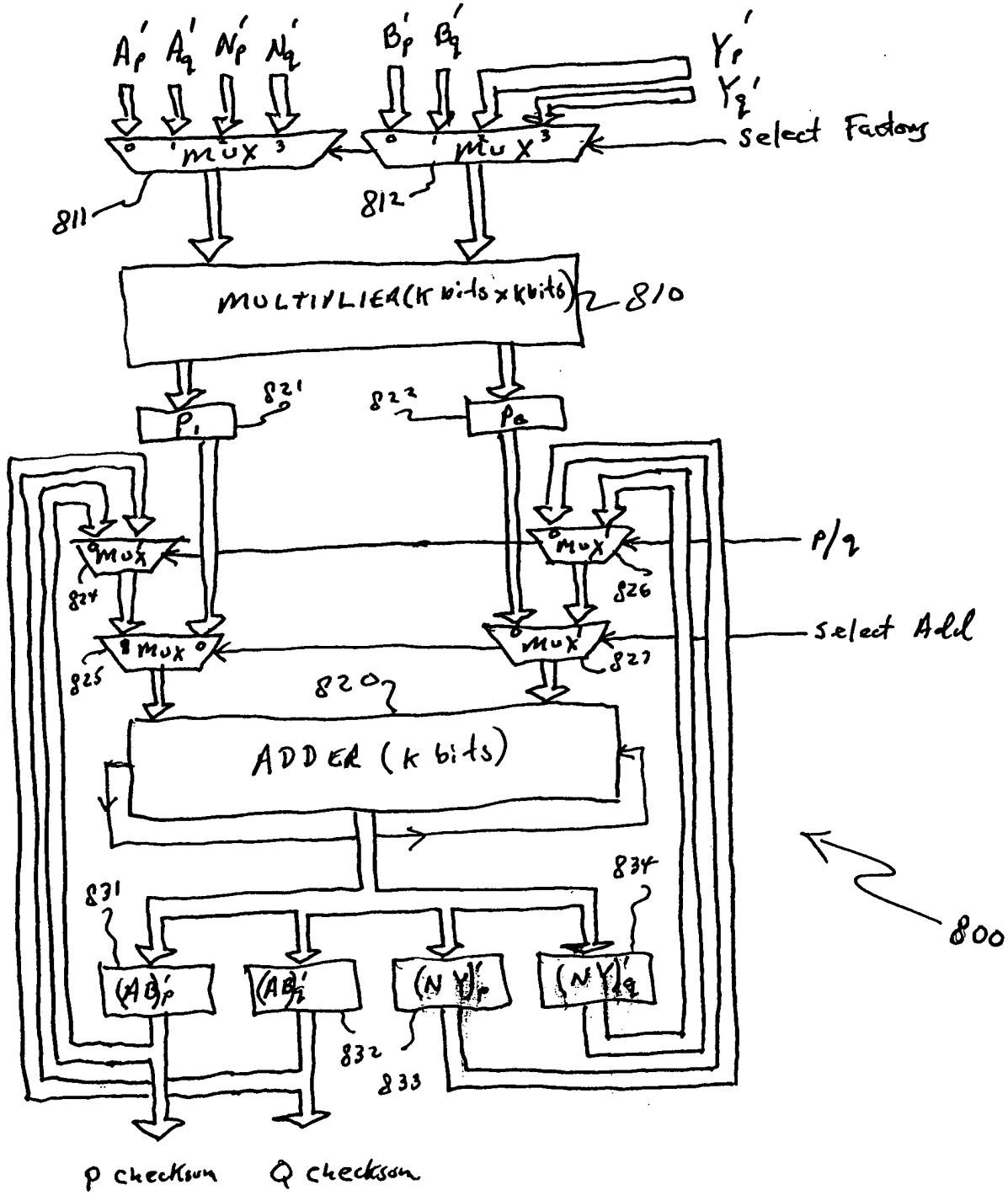
A'_p A'_q N'_p N'_q
B'_p B'_q
Y'_p
Y'_q
MUX 3
MUX 3
Select Factors
811
812
MULTIPLIER (K bits x K bits)
810
821
822
P/Q
824
826
Select Add
825
827
820
ADDER (K bits)
831
834
$(AB)'_p$
$(AB)'_q$
$(NY)'_p$
$(NY)'_q$
832
833
800
P Checksum
Q Checksum

Figure 25

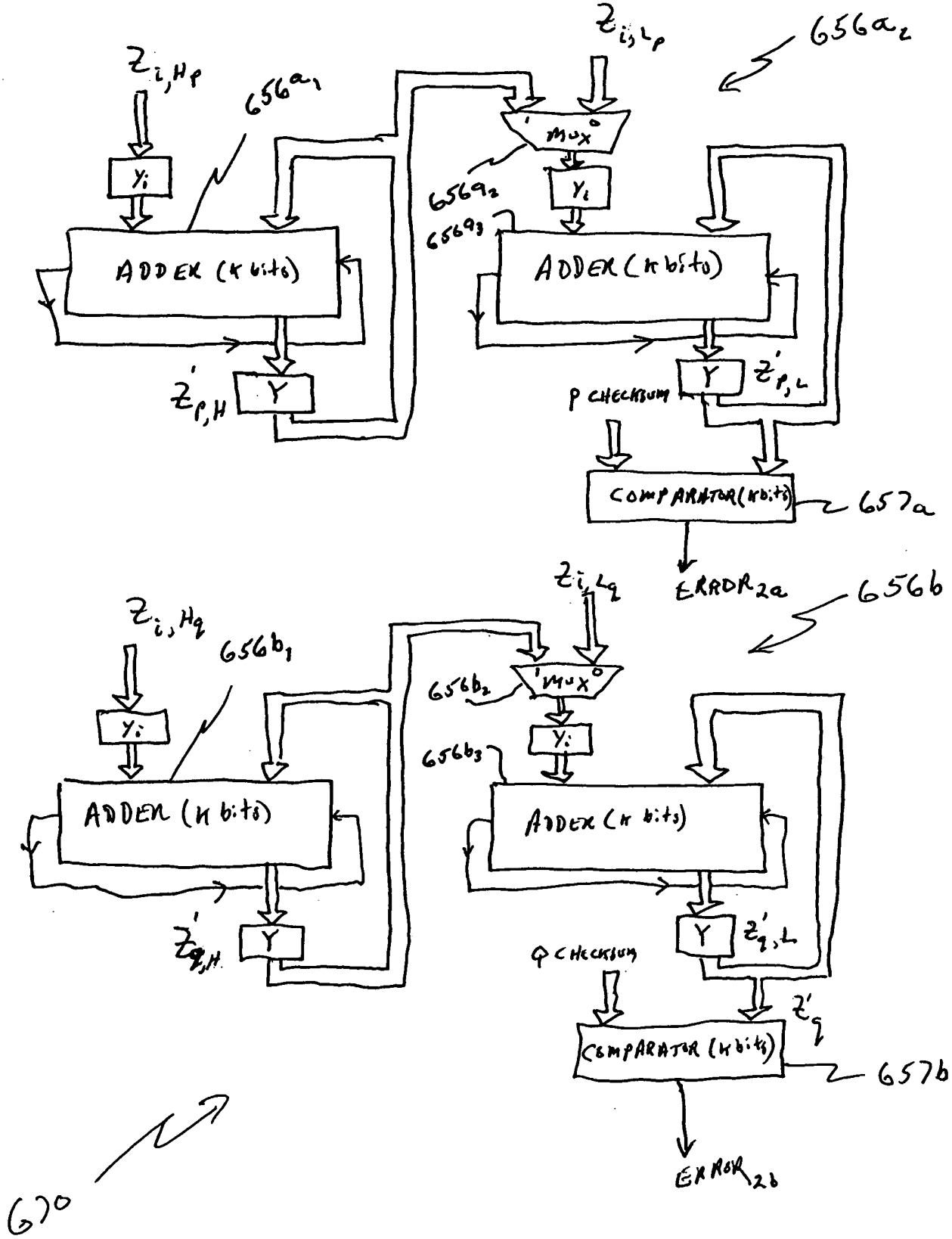
z_{i,L_p}
656a2
z_{i,H_p}
656a1
mux
Yi
656a3
ADDER (n bits)
$z'_{p,H}$
Y
$z'_{p,L}$
P CHECKSUM
COMPARATOR (n bits)
657a
ERROR2a
z_{i,L_q}
656b
z_{i,H_q}
656b1
656b2
656b3
ADDER (n bits)
$z'_{q,H}$
$z'_{q,L}$
Q CHECKSUM
z'_q
657b
ERROR2b
670

Figure 26